

Charles J. Nerko
Partner

May 5, 2022

VIA CM/ECF

The Hon. Diane Gujarati, U.S.D.J.
U.S. District Court for the Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: Pirozzi v. Fiserv Corp., Civil Action Number: 2:22-cv-902 (DG/AYS)

Dear Judge Gujarati:

We represent plaintiffs, the entities of Chef Pirozzi, and write to respond to defendants' pre-motion letter of April 28, 2022 setting forth the grounds for an anticipated motion to dismiss.

This action arises out of defendants' failure to safeguard plaintiffs' funds and defendants' attempts to conceal their security problems and shift blame to plaintiffs. As set forth in plaintiffs' amended complaint, in November 2020, plaintiffs contracted with defendants for merchant processing services to collect credit card payments plaintiffs' restaurant sales (the "Agreement") (Dkt. 23, ¶¶ 14-20). In August 2021, plaintiffs stopped receiving transfers of credit card receipts from defendants (Dkt. 23, ¶¶ 23-25). Upon discovery of the missing funds, defendants repeatedly misled and deceived plaintiffs as to the whereabouts of the missing funds and repeatedly promised funds would be returned in full to plaintiffs' bank account, but failed to do so (Dkt. 23, ¶¶ 24, 33-34, 43, 48, 52). Throughout plaintiffs' attempts to obtain the missing funds, defendants continued to collect credit card payments, and withhold them from plaintiffs. To date, plaintiffs have been unable to retrieve the entirety of the missing funds defendants collected (Dkt. 23, ¶ 24). Plaintiffs seek contract damages, contract rescission, and redress in tort for defendants' failure to maintain adequate security controls and for transferring plaintiffs' funds to an unknown third party.

Defendants' planned motion to dismiss ignores the amended complaint's detailed allegations of defendants' misconduct. At most, defendants raise disputed, fact-based defenses outside the pleadings that defendants may ultimately attempt to establish later on in the course of discovery. None of defendants' arguments is a basis to dismiss plaintiffs' well-pleaded claims.

First, plaintiffs have adequately alleged defendants are culpable for transferring plaintiffs' funds to an unauthorized individual (Dkt. 23, ¶¶ 15-24; 40-42). Defendants' speculation that plaintiffs failed to protect their password is not established in the pleadings and raises a sharply disputed, fact-based defense. Contrary to defendants' pre-motion letter (Dkt. 27, p. 1), plaintiffs do not admit that they failed to maintain the security of their account. Rather, plaintiffs allege that they did not make any changes to their account information (Dkt. 23, ¶¶ 22, 31, 40-42). Thus, defendants have not established that the hack resulted from plaintiffs' conduct. To the contrary, the amended complaint plausibly alleges that defendants lied about having proper security controls

in place (Dkt. 23, ¶¶ 20, 72-77, 147-148). This is confirmed by Fiserv, Inc.'s SEC Form 10-K, which admits the problems with defendants' security controls:

We expect that unauthorized parties will continue to attempt to gain access to our systems These events could create costly litigation [and] significant financial liability.... [W]e cannot be certain that the security measures and procedures we have in place to detect security incidents and protect sensitive data, including protection against unauthorized access and use by our employees, will be successful or sufficient to counter all current and emerging ... risks and threats. See <https://newsroom.fiserv.com/node/46626/html>.

The "unauthorized access and use by our employees" defendants concede is their employees' theft from defendants' own customers—which plausibly occurred here. Indeed, a district court recently held that another Fiserv customer adequately alleged that Fiserv's security failures were sufficiently serious to state contract, tort, and punitive damages claims. See *Bessemer Sys. FCU v. Fiserv Sols., LLC*, 472 F. Supp. 3d 142 (W.D. Pa. 2020). Similarly, a state appellate court held that yet another Fiserv customer alleged Fiserv's security was grossly negligent. See *Copper Basin FCU v. Fiserv Sols., Inc.*, 2013 WL 3421916, at *4-5 (Tenn. Ct. App. July 3, 2013) (unpublished).

Second, plaintiffs have adequately stated tort claims for the misconduct alleged in the amended complaint because: (1) these claims do not seek the benefit of any contractual bargain, but redress for defendants' independent, non-contractual legal duties (e.g., under bailment) to not provide plaintiffs' assets to an unauthorized third party; (2) plaintiffs adequately allege that the Agreement does not govern because the Agreement was procured by fraud, is unenforceable, and is subject to rescission; and (3) not all plaintiffs and defendants are in contractual privity.

In similar circumstances involving Fiserv's failure to implement security controls to prevent fraud, a district court applying New York contract law found the plaintiff adequately alleged contract and tort claims against Fiserv. See *Bessemer*, 472 F. Supp. 3d at 166. Further, California law (where plaintiffs are located and the injury occurred) recognizes a negligence claim for a lack of due cybersecurity that enables a "follow-on injury" by a third-party fraudster. See *Fraser v. Mint Mobile*, 2022 U.S. Dist. LEXIS 76772, at *6-11, *17-21 (N.D. Cal. Apr. 27, 2022).

Third, defendants' other objections to plaintiffs' claims lack merit:

- **Breach of Privacy Policies.** Plaintiff adequately alleged defendants' Privacy Policies are contracts or alternatively, detrimentally relied on and enforceable under promissory estoppel (Dkt. 23, ¶¶ 80-86). The merger clause in Section 45.6 of the Agreement providing it "constitutes the entire Agreement *between the parties* with respect *to the subject matter* thereof, and supersedes any *previous agreements and understandings*" does not vitiate the Privacy Policies because they (1) concern a different subject matter; (2) involve different parties; and (3) are not "previous agreements and understandings," negated by the merger clause, because the Privacy Policies are contemporaneous and/or subsequent agreements.

- **Fraud.** Plaintiffs' amended complaint adequately alleges that defendants purposely misled plaintiffs in a myriad of ways, and such allegations successfully make out a claim for fraud. Plaintiffs allege in detail that defendants made a series of misrepresentations and promises to provide proper security and return the missing funds, which were relied on by plaintiffs to their detriment (Dkt. 23, ¶¶ 95-101). Defendants' conduct was designed to string plaintiffs along with false promises that the funds would be returned to maintain plaintiffs as customers, continue to charge membership fees, and deter and frustrate plaintiffs from their own recovery efforts (Dkt. 23, ¶ 100). This misconduct is distinct from the Agreement. *See Bessemer, supra*.

- **Negligence.** Plaintiffs adequately alleged that defendants had a legal duty to protect plaintiffs from risk of identity theft and fraud (Dkt. 23, ¶¶ 121-129). This duty is independent of the contract and not barred by the economic loss doctrine. *See AMBAC Assur. Corp. v. United States Bank Nat'l Ass'n*, 328 F. Supp. 3d 141, 160 (S.D.N.Y. 2018) (denying motion to dismiss based on economic loss rule where plaintiff sufficiently alleged that it was harmed as the result of the breach of a legal duty independent of the breach of a contractual obligation); *Fraser, supra*.

- **Indemnification.** The amended complaint does not allege a pure inter-party claim given defendants' contention that a third party stole the funds. Further, plaintiffs have sufficiently pleaded intentional misconduct or gross negligence, as recognized by courts when defendants have caused other fraud losses based on their failure to implement reasonable security controls. *See Bessemer and Copper Basin, supra*; *see also Tillage Commodities Fund, L.P. v. SS&C Techs., Inc.*, 58 N.Y.S.3d 28, 30 (App. Div. 2017) (gross negligence claim stated based upon defendant processing fraudulent requests to transfer plaintiff's funds); *Roth v. Black Star Publ'g Co.*, 658 N.Y.S.2d 59, 61 (App. Div. 1997) (exculpatory agreement held unenforceable; "in the case of a bailment, the failure to return the object bailed is prima facie evidence of gross negligence").

- **Aiding and Abetting.** Knowledge of the fraud is alleged by defendants speaking to the fraudster to approve his/her illicit transfer of plaintiffs' funds. Also, defendants' SEC filing, *supra*, confirms defendants foresee their weak security will lead to "significant financial liability" because their own employees can misuse "sensitive data" (e.g., plaintiffs' password) to steal.

- **Declaratory Judgment on Unenforceability of Damages Waiver and Limitation of Liability.** *First*, a district court has previously rejected defendants' arguments, holding that a Fiserv customer adequately alleged similar provisions were unenforceable under New York's public policy. *See Bessemer*, 472 F. Supp. 3d at 182. *Second*, plaintiffs adequately alleged that defendants waived these provisions by making repeated independent promises to return plaintiffs' missing funds. *See TSS-Seedman's, Inc. v. Elota Realty Co.*, 72 N.Y.2d 1024 (1988) (party's conduct waived contract terms, including a nonwaiver clause). *Third*, these provisions of the Agreement are inapplicable to defendants' breaches of the Privacy Policies, which are separate and independent contracts.

Respectfully submitted,

Copy to: All counsel (by ECF)

/s/ Charles J. Nerko